REMARKS

By the foregoing, Claims 1, 11, and 18 have been amended, no claims have been canceled, and Claims 19-31 have been added. Claims 1-31 are pending in the application.

Initially, the Examiner is thanked for initialling and returning the PTO/SB/08A submitted by the Applicants on May 20, 2004.

Page 2 of the Office Action sets forth a rejection of independent claims 1, 11, and 18, and dependent claims 2-10 and 12-17 as being anticipated under 35 U.S.C. § 102(e) by Patent Application Publication 2004/0015694A1 to DeTreville.

Independent claim 1 is directed to a central processing unit including means for processing computer instructions comprising means for receiving computer instructions and means for executing computer instructions; a secure memory unit coupled to said processing means, said secure memory unit having one or more resident security check programs for determine whether the computer has been tampered with. When said means for processing information receives a secure attention instruction through said receiving means said means for executing computer instructions executes the security check program by retrieving its instructions from the secure memory.

Claim 1 has been amended to recite that the resident security check programs determine whether the computer has been tampered with.

DeTreville is directed to a system for authenticating an open computer system with a

portable IC device. As discussed in DeTreville, an "open" computer system is one that is publicly accessible, for example, a compuer in a hotel room, a kiosk, or a shopping mall. In particular, DeTreville discloses a system that allows an an open computer system to provide certificates of authenticity to the "smart card" before the smart card reveals private or other sensitive information to the applications executing on the system. See para [0010] - [0012]. As discussed in para [0011], the applications running on the computer are authenticated using an authenticated boot methodology. Para [0036] further describes that "one or more of the applications running on the computer are authenticated to IC device 116". Paragraph [0037] explains two methods. One way to support such authentication is referred to as "authenticated boot methodology", the operating system on the computer is able to prove its identity to the microprocessor and thereby certify that it is trusted". Another way is to use a curtaining methodology, wherein "trusted applications can be executed in a secure manner regardless of the trustworthiness of the operating system".

According to paragraph [0104] of DeTreville, "The trusted code that is permitted to perform secure operations and to handle secret data is called curtained code. In other systems, such code must be executed within a privileged operating mode of the processor not accessible to non-trusted software, or from a separate secure processor. In the present invention, however, curtained code can only be executed from particular locations in memory. If this memory is made secure against intrusion, then the curtained code can be trusted by third parties. Other features restrict subversion through attempts at partial or modified execution of the curtained

code."

The Office Action indicates that DeTreville's curtained code is believed to correspond to the claimed security check program. However, there is no disclosure in DeTreville that the curtained code determines whether the computer has been tampered with. Instead, the curtained code allows execution of code within the curtained region whether or not the computer has been tampered with, as long as the entry points in an outer ring of the curtained region is secure. According to DeTreville at [0037], "using the curtaining methodology, trusted applications can be executed in a secure manner regardless of the trustworthiness of the operating system. A security manager coordinates such execution, and can provide certificates proving that particular applications are executing in a secure manner." Thus, the curtaining methodology allows programs to run within a curtained memory ring regardless of the status of the computer areas outside the ring.

Accordingly, the DeTreville curtained code cannot correspond to the claimed security program that determines whether the computer has been tampered with, and DeTreville therefore does not discluse all the features set forth in amended claim 1. Reexamination and allowance of Claim 1 is requested.

Claim 1 has also been amended to delete language not believed to be necessary for patentability stating that the means for executing computer instructions interrupts the instructions it is executing. New claim 22 depends from claim 1 and includes this feature that was previously set forth in claim 1.

For at least these reasons, Claim 1 is believed to be allowable over DeTreville, and withdrawal of the rejection of Claim 1 is respectfully requested.

Independent claim 18 has also been amended to include the feature that a security check program that determines whether the computer has been tampered with, and is believed to be allowable for at least the same reasons that claim 1 is allowable.

Independent claim 11, directed to a central processing unit, has been amended to include the feature that upon the receipt of a secure attention instruction by the CPU, the CPU executes one or more check programs from the secure memory unit for determining whether the computer has been tampered with and, upon the execution of the security check program if the result of the check program is satisfactory, the cryptographic check key is used to authenticate the result values transmitted to the source of the secure attention instruction.

As discussed in the paragraphs above, there is no disclosure in DeTreville of a check programs from the secure memory unit for determining whether the computer has been tampered with. Accordingly, withdrawal of the rejection of claim 18 is requested.

Although the dependent claims are believed to be allowable for at least the same reasons that claims 1, 11, and 18 are allowable, a few comments are provided to further prosecution.

Dependent claim 19 recites that the system determines whether a deceptive interpreter is present. Dependent claim 20 recites that the security check programs determine whether at least one of malicious instructions, viruses, deceptive interpreters, and Trojan horses are present.

DeTreville does not disclose a security check program having either of these features. The Office Action indicates that DeTreville's curtained code is believed to correspond to the claimed security check program. For example, DeTreville at [0104] defines curtained code as the trusted code that is permitted to perform secure operations and to handle secret data. DeTreville does not disclose that the curtained code determines whether at least one of malicious instructions, viruses, deceptive interpreters, and Trojan horses are present, or whether deceptive interpreters are present.

Claims 19 and 20 are allowable over DeTreville for at least these additional reasons.

Claim 21 sets forth that following the security check, the processing means transmits results of the security check program and transmits an authentication value from the secure memory unit and, and an incorrect or absent authentication value indicates the presence of a deceptive interpreter. DeTreville does not disclose at least this additional feature.

New claims 22-31 set forth additional subject matter to which the applicants are believed to be entitled, directed to subject matter not found in the cited references.

In view of the foregoing amendments and remarks, reconsideration, reexamination, and allowance of the present application is respectfully requested.

Should there be any questions regarding this Amendment, or the application in general, the examiner is cordially invited to contact the undersigned at the number listed below.

Respectfully submitted,

Date: April 26, 2005

By: Sally A Ferrett

Sally A. Ferrett
Registration No. 46,325

Naval Research Laboratory
Office of Associate Counsel (Patents)
4555 Overlook Ave., SW 20375
(202) 404-1551